

Chapter 10

Hierarchy Similarity Analyser: An Approach to Securely Share Electronic Health Records

Shalini Bhartiya
IITM New Delhi, India

Deepti Mehrotra
Amity University Noida, India

Anup Girdhar
Sedulity Groups, India

ABSTRACT

Health professionals need an access to various dimensions of Electronic Health Records (EHR). Depending on technical constraints, each organization defines its own access control schema exhibiting heterogeneity in organizational rules and policies. Achieving interoperability between such schemas often result in contradictory rules thereby exposing data to undue disclosures. Permitting interoperable sharing of EHRs and simultaneously restricting unauthorized access is the major objective of this paper. An Extensible Access Control Markup Language (XACML)-based framework, Hierarchy Similarity Analyser (HSA), is proposed which fine-grains access control policies of disparate healthcare organizations to achieve interoperable and secured sharing of EHR under set authorizations. The proposed framework is implemented and verified using automated Access Control Policy Testing (ACPT) tool developed by NIST. Experimental results identify the users receive secured and restricted access as per their authorizations and role hierarchy in the organization.

1. INTRODUCTION

The inclusion of electronic media in healthcare domain resulted in transformation of paper-based health records into Electronic Health Records (EHRs). These records are accessed from medical to non-medical users at the same time across multiple hospitals and other related organizations. These records possess a high level of sensitivity where the patient demands utmost care allowing only relevant and authorized

DOI: 10.4018/978-1-5225-9863-3.ch010

access of the records. Rules and policies are defined with respect to the roles and responsibilities of health providers. It may differ from hospital to hospital. With the heterogeneity involved in the organizational structure and access policies, sharing EHR increases the chance of confidentiality leakages and security breaches. Organizations, hospitals in this context, experience various challenges and security issues (Bhartiya & Mehrotra, 2014; Bai et al., 2014) in making the data available to the intended users.

In spite of similar roles of the users, the two hospitals may exhibit dissimilarity in their organizational hierarchies. Hence, to enable cross-organizational sharing of data, well-defined standards or mechanisms should be developed. The objective is to logically identify similarities between user's roles and authorities and make two disparate organizations interoperable. For ex. comparing two doctors, one in government hospital and the other in private hospital, their work distribution may not be the same and hence, the set of access rules must differ in both cases. A possibility exists where an access to the resource should be permitted to one and denied to other. The case reflects a huge challenge in determining and setting their access rights and privileges for secured sharing of sensitive EHR in spite of wide gap in their services.

Basically, sharing of EHR is dependent on how best the two systems can achieve interoperability. HL7 has been addressing interoperability problems in sharing or exchanging EHRs for over two decades now. It (HL7 Standards, 2015; HL7 Evolution, 2010) provides a framework for exchange and sharing of EHRs for seamless integration between disparate healthcare organizations. The Standard is broadly divided into two categories – Version 2 (V2) and Version 3 (V3). Fast Healthcare Interoperability Resources Specification (FHIR), Release 1 (HL7 FHIR, 2015) combines the best features of HL7's V2, V3 and CDA product lines. It is a standard for exchanging healthcare data electronically. It simplifies implementation without compromising information integrity. Integrity is complemented with confidentiality and availability of data.

Interoperable sharing of EHRs exhibits another challenge -maintaining the confidentiality and privacy of sensitive health information without compromising its availability to the health providers. NIST (NIST 800-53, 2013) in collaboration with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DoD), and the Committee on National Security Systems (CNSS) is establishing a unified information security framework for the federal government. This framework is said to provide a strong base for mutual acceptance of authorization decisions and facilitate information sharing between disparate organizations.

An access control framework allocates the access rights and privileges on the resources. A typical deployment of an access control system is a combination of three logical components: an access control model (ACM), policies, and enforcement mechanisms. A logical access control system requires validating individual's roles and responsibilities for assigning the access rights on the data. As each system is autonomous specifying access control policies according to the user and resource hierarchy of the organization, collaborating such organizations often result in policy conflicts (Huang and Liu, 2009), matching of undefined attributes or rules, thus, imposing a threat to relevant and meaningful disclosure of the information. Support from industry standard access methods would enable the disparate EHR-systems to collaborate and expand access to the data for providing quality (de la Torre-Diez et al., 2012) and timely care to the patient. The Standards and Interoperability (S&I) Data Access Framework (DAF) Initiative outlines the standards and profiles necessary for clinicians, providers and healthcare professionals to gain access to patient data within an organization and across organizations. DAF addresses three basic challenges-Who is accessing data, what and how the data is accessed and why the data is accessed?

Figure 1 identifies the different environments of information access requirements with respect to interoperable healthcare domain. DAF proposes to implement interoperable data access through a

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/hierarchy-similarity-analyser/235313

Related Content

Dietary Management

(2020). *Diagnosing and Managing Hashimoto's Disease: Emerging Research and Opportunities* (pp. 215-240).

www.irma-international.org/chapter/dietary-management/243796

Designing a Framework of Ethnomedicinal Plant Knowledge Integration Using OSS

Piyali Das (2022). *Research Anthology on Recent Advancements in Ethnopharmacology and Nutraceuticals* (pp. 518-531).

www.irma-international.org/chapter/designing-a-framework-of-ethnomedicinal-plant-knowledge-integration-using-oss/289500

Design and Development of Real Time Patient Monitoring System with GSM Technology

Sindhu Suryanarayanan, Sreekala Manmadhanand N. Rakesh (2020). *Virtual and Mobile Healthcare: Breakthroughs in Research and Practice* (pp. 627-642).

www.irma-international.org/chapter/design-and-development-of-real-time-patient-monitoring-system-with-gsm-technology/235336

Treatment of Uterine Pathology: When Is Simple Hysterectomy Indicated?

Dimitrios Tsolakidis and Maria Lantzanaki (2021). *Handbook of Research on Oncological and Endoscopic Dilemmas in Modern Gynecological Clinical Practice* (pp. 305-320).

www.irma-international.org/chapter/treatment-of-uterine-pathology/260094

Falls in Elderly: A Hospital Reality Integrative Review

Tânia Patrícia Cabo Relíquias, Carmen Dolores Roque Agostinho and Maria do Céu Marques (2020). *Handbook of Research on Health Systems and Organizations for an Aging Society* (pp. 196-207).

www.irma-international.org/chapter/falls-in-elderly/238281